Appendix B - Example Policies & Procedures

This section contains sample policies for the NAS Division at NASA Ames Research Center. The last policy is a draft example that was written for a partnership with Cisco Systems.

The following documents are included in this section:

Sample Computer Usage Guidelines

I. Introduction

This document establishes computer usage guidelines for the <COMPANY NAME> Systems Division support staff in the course of their job duties on <COMPANY NAME> Computer Systems. These guidelines incorporate the elements of the <COMPANY NAME> Systems Division Special Access Agreement and the Acceptable Use Statement of <COMPANY NAME> Systems Division Computing Resources. These guidelines are intended to protect the rights and privacy of <COMPANY NAME> Systems Division clients as well as those of <COMPANY NAME> Systems Division support staff. Any Corporate Headquarters guidelines or policies will take precedence over these guidelines.

II. Other Applicable Guidelines/Policies

Members of the <COMPANY NAME> Systems Division support staff are required to abide by all the items outlined in the Acceptable Use Statement of <COMPANY NAME> Systems Division Computing Resources. In addition to being the guardians/supporters of the <COMPANY NAME> resources, members of the <COMPANY NAME> support staff also serve as examples of professionalism for the rest of the <COMPANY NAME> user community.

Many members of the <COMPANY NAME> Systems Division support staff have some level of special access. Special access is defined as having the password and privilege to use a special account (e.g., root) on a <COMPANY NAME> System Division computer or subsystem or to have privileges above and beyond those of normal users. The first time a member of the <COMPANY NAME> support staff requests special access, he/she is asked to read and sign the Special Access Guidelines Agreement. This agreement presents general guidelines for using special access in a responsible and ethical manner. The agreement also specifies behaviors and practices that are prohibited. All members of the <COMPANY NAME> support staff should reference the The Special Access Guidelines Agreement whenever they have a question regarding proper use of special access. The document may be accessed via <Company Name>info in the Misc_Info section, under the title sp.access.policy .Highlights of the guidelines are provided below.

III. Privacy of Clients Data/Information

There is one particular topic that is not covered in detail in either of the two documents discussed above. That topic is the privacy of clients files and information stored on/in <COMPANY NAME> Systems Division computers and resources. Sometimes during the normal course of their job, a member of the <COMPANY NAME> support staff will have a need to view a file belonging to another person. Some examples are: helping a client with a programming problem which requires access to the client's source program; helping a client resolve an electronic mail problem which requires viewing part of the client's mail message file. Whenever required to view a client's file in the course of helping that client, the consent of the client must be first obtained. In the case of resolving an electronic mail problem, in which the message has been returned to the postmaster account, consent is also implied. However, in all cases the client must be advised that his/her file(s) must be viewed/accessed to assist them.

When assisting <COMPANY NAME> clients, members of the <COMPANY NAME> Systems Division Support Staff should use the following guidelines:

* Use and disclose the clients data/information only to the extent necessary to perform the work required to assist the client. Particular emphasis should be placed on restricting disclosure of the data/information

to those persons who have a definite need for the data in order to perform their work in assisting the client.

* Do not reproduce the client's data/information unless specifically permitted by the client.
* Refrain from disclosing a client's data/information to third parties unless written consent is provided by the client.
* Return or deliver to the client, when requested, all data/information or copies there of to the client or someone the designate.

IV. Proprietary Information

Due to the nature of <COMPANY NAME> Systems Division, there is a large potential for having proprietary information stored on/in <COMPANY NAME> computers and resources. Information that would be considered proprietary would be vendor source code, benchmark programs, benchmark results, scientific codes and data sets. Since members of the <COMPANY NAME> support staff will have full access to the <COMPANY NAME> systems and resources, they will potentially have access to proprietary information. Members of the <COMPANY NAME> support staff are responsible for ensuring that all proprietary information is protected from disclosure or modification. When dealing with proprietary information, members of the <COMPANY NAME> support staff should use the following guidelines:

* Ensure appropriate measures are in place for protecting proprietary information.
* Do not attempt to access proprietary information for which you have not been given authorization.
* Do not make copies of proprietary information unless specifically permitted by the owner of the information.
* Refrain from disclosing to third parties the types of proprietary information you can access.

V. Security Investigations

If during the course of their regular duties, a member of the <COMPANY NAME> support staff discovers evidence of a violation of the Acceptable Use Statement for <COMPANY NAME> Systems Division Computing Resources, he or she must notify the <COMPANY NAME> Data Processing Installation Computer Security Officer (DPI-CSO), the <COMPANY NAME> Computer Security Analyst (CSA) or the <COMPANY NAME> Systems Division Chief. If the DPI-CSO, CSA or the <COMPANY NAME> Division Chief determines there is probable cause to believe a violation has occurred, additional investigation will be authorized. Any additional investigation will normally be performed by the <COMPANY NAME> CSA or someone else designated by the DPI-CSO or the <COMPANY NAME> Division Chief. Members of the <COMPANY NAME> Systems Division support staff should not begin an investigation of a client without receiving authorization from the proper person.

If you are requested to participate in an investigation of a client, or you must view a client's files (after receiving consent) during the normal course of your job duties, you must be careful not to disclose information about that client or the contents of the client's files to other people. Information concerning the client should only be disclosed to the DPI-CSO, CSA, the <COMPANY NAME> Division Chief or to a law enforcement agency. It is also very important to keep a detailed record of all actions when investigating an allegation of improper use.

VI. Summary of Guidelines

To summarize, please follow these guidelines:

* Read and follow the Acceptable Use Statement of <COMPANY NAME> Systems Division Computing Resources.
* Read and follow the <COMPANY NAME> Systems Division Special Access Agreement.
* Do not inspect a client's files without consent of the client or the proper authorization.
* Inform the proper people when you feel there is evidence of a possible violation.
* When performing an investigation on a client or system which involves viewing client's private files/data/information, keep a detailed record of why the investigation was initiated and what actions you took.

Concurrence:

Approved By:

Sample Acceptable Use Statement

The following document outlines guidelines for use of the computing systems and facilities located at or operated by (<COMPANY NAME>) The definition of <COMPANY NAME> Systems Division and computing facilities will include any computer, server or network provided or supported by the <COMPANY NAME> Systems Division. Use of the computer facilities includes the use of data/programs stored on <COMPANY NAME> Systems Division computing systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the <COMPANY NAME> Systems Division. The "user" of the system is the person requesting an account (or accounts) in order to perform work in support of the <COMPANY NAME> program or a project authorized for the <COMPANY NAME> Systems Division. The purpose of these guidelines is to ensure that all <COMPANY NAME> users (scientific users, support personnel and management) use the <COMPANY NAME> Systems Division computing facilities in a effective, efficient, ethical and lawful manner.

<COMPANY NAME> accounts are to be used only for the purpose for which they are authorized and are not to be used for non-<COMPANY NAME> related activities. Unauthorized use of a <COMPANY NAME> account/system is in violation of Section 799, Title 18, U.S. Code, and constitutes theft and is punishable by law. Therefore, unauthorized use of <COMPANY NAME> Systems Division computing systems and facilities may constitute grounds for either civil or criminal prosecution.

In the text below, "users" refers to users of the <COMPANY NAME> Systems Division computing systems and facilities.

1.The <COMPANY NAME> Systems Division computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a <COMPANY NAME> Systems Division computing system. Information is considered "classified" if it is Top Secret, Secret and/or Confidential information which requires safeguarding in the interest of National Security.

2. Users are responsible for protecting any information used and/or stored on/in their <COMPANY NAME> accounts. Consult the <COMPANY NAME> User Guide for guidelines on protecting your account and information using the standard system protection mechanisms.

3. Users are requested to report any weaknesses in <COMPANY NAME> computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting <COMPANY NAME> User Services or by sending electronic mail to security@company.com4. Users shall not attempt to access any data or programs contained on <COMPANY NAME> systems for which they do not have authorization or explicit consent of the owner of the data/program, the <COMPANY NAME> Division Chief or the <COMPANY NAME> Data Processing Installation Computer Security Officer (DPI-CSO).

5. Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

7. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

8. Users shall not make copies of system configuration files (e.g/etc/passwd) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.

9. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized <COMPANY NAME> user access to a <COMPANY NAME> resource; obtain extra resources, beyond those allocated; circumvent <COMPANY NAME> computer security measures or gain access to a <COMPANY NAME> system for which proper authorization has not been given.

10. Electronic communication facilities (such as Email or Netnews) are for authorized government use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on <COMPANY NAME> systems/

Users shall not down-load, install or run security programs or utilities which reveal weaknesses in the security of a system. For example, <COMPANY NAME> users shall not run password cracking programs on <COMPANY NAME> Systems Division computing systems.

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the <COMPANY NAME> user and the <COMPANY NAME> DPI-CSO and will result in short-term or permanent loss of access to <COMPANY NAME> Systems Division computing systems. Serious violations may result in civil or criminal prosecution.

I have read and understand the <COMPANY NAME> Systems Division computing systems Use Ethics Statement for use of the <COMPANY NAME> computing facility and agree to abide by it.

Signature: Date:

Sample Special Access Policy

This policy provides a set of requirements for the regulation and use special access on the NPSN systems. This policy will provide a mechanism for the addition and removal of people from the special access database and a mechanism for periodic reviews of the special access database.

The special access account UID's which are covered in this policy include: (some generic accouints)

The documents to be included as part of this policy are the Special Access Request form and the Special Access Guidelines agreement.

A. Policy For Regulation of Special Access Accounts:

1. Special access on <COMPANY NAME> systems is maintained and monitored, via the Special Access database, by both <COMPANY NAME> Operations and the <COMPANY NAME> Security Officer and/or assistant.

2. Passwords for special access accounts are changed on a regular basis, as determined by <COMPANY NAME> Operations Manager and/or the <COMPANY NAME> Security Officer.

3. Individuals authorized to receive special access passwords are required to pick up and sign for said passwords each time the passwords are changed.

4. Special access is only provided to individuals who need said access to perform their job.

5. Any misuse of special access privileges must be reported to the <COMPANY NAME> Security Officer within 24 hours.

6. UID zero account are to be strictly limited and monitored by the <COMPANY NAME> Security Officer and/or the <COMPANY NAME> Operations Manager. An example of a current UID zero account is the SGI field engineer's account.

7. Persons requesting special access must follow all procedures outlined in section B of this document.

8. Persons who misuse their special access privilege can have said access revoked as outlined in Section D of this document.

9. Contents of the special access database is reviewed on a periodic basis as outlined in Section C of this document.

10. All persons who currently (prior to the approval of this policy) have special access are required to submit a completed Special Access Request form and a signed Special Access Guidelines agreement.

B. Policy for Acquiring Special Access:

1. All persons requesting special access must complete a Special Access Request form (see attachment 1). The instructions for completing the form are listed on the back. A separate form must be completed for each separate subsystem and/or branch signature that is needed. The appropriate people for approval signatures are also listed on the back of the form.

2. All persons requesting special access must read and sign the Special Access Guidelines Agreement (See attachment 2). This agreement discusses the do's and don'ts of using special access. Once a person signs the agreement he/she is then bound to abide by its contents. A copy of the signed agreement will be provided to the person for his/her personal records. The signed originals will become a part of the that person's account/access file.

3. Any person refusing to sign the Special Access Guidelines Agreement will not be provided special access.

4. Persons with special access are to inform the <COMPANY NAME> Security Officer and/or <COMPANY NAME> Operations Officer if their special access requirements change.

C. Policy for Performing a Periodic Review of the Special Access Database:

A review of the special access database will be made on a regular basis or as determined by the <COMPANY NAME> Security Officer. The review process will involve the following steps:

1. Two reports will be generated from the special access database. One report lists special access by system and access type. The second report lists the access by person (i.e., for each person, all access given to that person is listed).

2) The two reports are distributed to all Subsystem managers, CSC Section managers and the Lead System Analyst for each system. Each person reviews the list (or appropriate part of) to determine if any changes should be made.

3)All persons requesting changes to the database must forward their comments to the <COMPANY NAME> Security Officer.

4) Should anyone determine that an individual needs to be added to other special access groups, that individual must submit a Special Access Request form requesting additional access.

5) If there are any deletions to be made to the database, the proper procedure outlined in Section D must be followed.

D. Policy for Removing People From the Special Access Database:

1. A person may be removed from the special access database for one of three reasons:
   - the person no longer works at <COMPANY NAME>
   - the person no longer needs special access due to a change in job duties
   - the person has violated the Special Access Guidelines agreement.

2. A person may be removed from the special access database at any time as determined by the <COMPANY NAME> Security Officer and/or appropriate Branch Chief or during one of the regular reviews of the database as described in Section C.

3. The procedures for removing a person from the special access database are as follows:

Case One: Person no longer works at <COMPANY NAME>

1. Fill out a Special Access Request form specifying the removal of all access.
2. Have <COMPANY NAME> Security Officer, or his designated assistant, sign form.
3. Update database and change affected password(s) within five working days.
4. Notify appropriate Branch Chief about deletion(s).

Case Two: Person no longer needs special access due to a change in job duties

1) Fill out Special Access Request Form specifying the removal of appropriate access(es).
2) Have employee's manager sign form. (**NOTE** This is for information only)
3) Have appropriate Subsystem Manager and/or Branch Chief sign form.
4) Update database during the next change of passwords.

Case Three: Person violated the Special Access Guidelines agreement

1) Appropriate people (i.e., Subsystem manager, <COMPANY NAME> Security Officer, Branch Chief) must decide if the violation constitutes removal of all special access of that person or just the special access involved.
2) Fill out Special Access Request Form specifying removal of appropriate access.
3) Have employeeÕs manager sign form.
4) Have appropriate Subsystem Manager and Branch Chief sign form.
5) Update database and change passwords within 24 hours.

Approved by:

Concurrence:

Sample Special Access Guidelines Agreement

This agreement outlines the many do's and do not's of using special access on NAS computers. Special access is defined as having the privilege and password to use one or more of the following accounts: () . The NAS environment is very complex and dynamic. Due to the number and variety of computers and peripherals, special access must be granted to numerous people so the NAS facility can be properly supported. People with special access must develop the proper skill for using that access responsibly.

The Special Access Guidelines have been developed to help people to use their special access in a responsible and secure manner. All persons requesting special access must read and sign this agreement. Anyone refusing to sign this agreement will not be granted the special access that they requested.

General Guidelines

1. Be aware of the NAS environment.

The NAS facility is a highly specialized facility containing a large number of computers of different configurations. Many daily system tasks have been automated by the use of software tools. Be aware of the "NAS Way" of doing system tasks.

2. Always log on systems where you have an account as yourself and then "su" to the appropriate UID. Any action done under a special access account should have an audit trail. When possible (i.e. on systems where you have a personal account) log into a system using your own account and then "su" to the needed UID.

3. Use special access only if necessary.

Many system tasks require the use of root or other special access. However, there are many tasks that can be done without the use of special access. When at all possible use regular accounts for trouble-shooting and investigating.

4. Document all major actions and/or inform appropriate people.

Documentation provides a method to analyze what happened. In the future, others may want to know what was done to correct a certain problem. The Lead System Analyst or Subsystem Manager is to be informed BEFORE any changes are made to system specific or configuration files.

5. Have a backup plan in case something goes wrong.

Special access, especially root, has a large potential for doing damage with just a few keystrokes. Develop a backup plan in case something goes wrong. You must be able to restore the system to its state before the error occurred.

6. Know whom to turn to if problems arise.With the use of special access, situations arise that have never come up before. Although NAS has many written procedures, they do not cover every circumstance possible. If any doubt exists about how you should proceed on a problem, then ask for assistance. Know whom to ask.

Specific Do not's of Special Access

1. Do not share special access passwords with anyone.
2. Do not write down the special access passwords or the current algorithm.
3. Do not routinely log onto a system, for which you have an account, as "root" or any other special access account.
4. Do not read or send personal mail, play games, read the net news or edit personal files using a special access account.
5. Do not browse other user's files, directories or E-mail using a special access account.
6. Do not make a change on any system that is not directly related to your job duties. The NAS System Administration Handbook states "The Lead System Analyst is responsible for approving all changes to the systems(s) of his/her responsibility. No changes are to be made to any system configuration file or executable file with prior approval of the Lead System Analyst". Making a change AND then informing the LSA is considered a violation of this guideline.
7. Do not use special access to create temporary files or directories for your own personal use.

I certify that I have read the above guidelines and will use this special access in accordance with NAS guidelines and policies. Misuse of any special access privilege will result in removal of that access.

Signature: Date:

Sample Network Connection Policy

This policy describes the requirements and constraints for attaching a computer to the <companyh name> work. All computers installed on company.com network fall under the authority and responsibility of the Data Processing Installation Computer Security Officer (DPI-CSO) and as such they must meet the minimum security requirements <company name> regulations and policies. The security requirements and practices at <COMPANY NAME> are outlined in Chapter 13 of the <COMPANY NAME> System Administration Guide (available on-line at <some random url

The intent of this policy is to ensure that all systems installed on the <COMPANY NAME> network are maintained at appropriate levels of security while at the same time not impeding the ability of <COMPANY NAME> users and support staff to perform their work.

As of December 1992, the <COMPANY NAME> DPI-CSO is () and the <COMPANY NAME> CSA is () Questions or concerns regarding <COMPANY NAME> security can be sent to the mail alias "security@company.com."

1. System Types

1.1. Secured Systems

A Secured system is fully supported by the <COMPANY NAME> support staff,who ensure it meets all of the <COMPANY NAME> security requirements outlined in Chapter 13, Security, in <COMPANY NAME> System Administration Guide and any requirements outlined in this policy.

1.2. Unsecured Systems

An unsecured system is not supported by the <COMPANY NAME> support staff. An unsecured system is installed on a separated subnet and is part of a specific subdomain of domain. The subnet is created by the use of a router and TCL box for each unsecured system location or by the use of a separate network and router in each of the equipment rooms.

The primary user of the system, or someone they designate, is responsible for the integrity of the system, and will ensure the system meets the minimum security requirements. Unsecured systems are treated as untrusted hosts by the secured systems and are viewed, as much as possible, like any other system on the Internet. Unsecured systems are not provided all of the services that are provided to secured systems. Services that will be provided are: lpr printer support and network table updates. The services that will not be provided are client partition support (e.g. /pub/sparc or /pub/iris4d_irix4) and the ability to remote mount, via NFS, partitions secured systems.

The approval for an unsecured classification is made by the DPI-CSO. When requesting a classification of "unsecured", the primary user of the proposed unsecured system may need to provide additional funds for the hardware needed to install the system on the unsecured subnet and must agree on what security features, if any, will be installed on the proposed unsecured system. The DPI-CSO is responsible for approving that the agreed security measures are adequate and the primary user is responsible for ensuring that the agreed security measures are put in place and are operational. Any security incident occurring on a secured or unsecured system on the <COMPANY NAME> network can adversely effect the security of other <COMPANY NAME> systems or impact the reputation of the <COMPANY NAME> facility, and as such, will be resolved under the direction of the <COMPANY NAME> DPI-CSO and the <COMPANY NAME> CSA.

2. Minimum Network Hook-up Requirements for Secured Systems

The requirements listed below are the minimum requirements which must be satisfied before a new host can be installed on the network as a <COMPANY NAME>-secured system.

2.1. Designation of Support Group or Responsible Person

Each computer attached to the <Company Name>.nasa.gov network must have an assigned group or individual who provides full support for the system and is responsible for ensuring the requirements of this policy are met. In addition, the responsible person or group ensures that the security of the system is maintained by installing needed security patches and security checking programs. The person or group who is responsible for support must have full access to the system. If the <COMPANY NAME>-secured system is not to be supported by the support staff, then the <COMPANY NAME> security staff must be notified and full access to the system (including roo access) is provided to the

<COMPANY NAME> Computer Security Analyst (CSA). Since a security incident on a <COMPANY NAME>-secured system may have an impact on other <COMPANY NAME>-secured systems, the responsible person or group must be reachable 24 hrs/day, 7 days/week in the event of a major security incident.

2.2. Notification of New System Installation

The appropriate personnel must be notified each time a new host is added to the company.com network. The group of appropriate personnel includes the DPI-CSO, the CSA, the <COMPANY NAME> Network support group, and in most cases, the <COMPANY NAME> WKS support group. Prior to installation on the network, a valid IP address number must be assigned by the Network Operations Group. An IP address number can be obtained by sending email or leaving voice mail for the Network Operations Group. As part of the IP address request, the requestor must specify the new host as <COMPANY NAME>-secured or unsecured. If the system is designated as "unsecured", the Network Operations Group must first verify the request with the DPI-CSO prior to assigning a network IP address. The support status of the systems (e.g. "<COMPANY NAME>-secured" or "unsecured") must be included when the<Company Name>.nets newsgroup, by the Network Operations Group. In addition to posting a notice to <Company Name>. newsgroup, the Network Operations Group will be responsible for sending an email message, containing the same information as the news posting, to security mail alias. All other appropriate <COMPANY NAME> support personnel (e.g., WKS group, HSP group, etc) will be responsible for reading the <Company Name>.nets news group on a regular basis (e.g., daily or several times a week).

2.3. Required Account(s)

Each <COMPANY NAME>-secured computer attached to company.com network must s and netops system account to allow members of the support team access to the system in the event of a problem or to perform routine system functions.

2.4. Root Access

Passwords to special privileged accounts for all computers attached to the company.com network must be documented in a secure location. The and other special access passwords for secured systems are assigned by the <COMPANY NAME> CSA and are stored in the <COMPANY NAME> password database. All password changes for the root and other support accounts must be reported to the <COMPANY NAME> CSA within two working days. Periodic system access checks will be made to ensure conformance. All accounts on the system must have a password.

2.5. Standard <COMPANY NAME> UIDS

All accounts installed on systems on company.com network must be assigned a valid UID which is unique to that account and user. Valid <COMPANY NAME> UIDs can be obtained from the accounts staff within User Services and can be reached via email at account#company.com

2.6. Standard <COMPANY NAME> Network Parameters

All hosts in the company.com domain must obtain a valid network number from the Network Operations group. <COMPANY NAME> uses a subnetted class B address, netmask 255.255.255.0. The configured broadcast address for all <COMPANY NAME> hosts uses all ones for the host portion (e.g. 129.99.23.255). No host on the network should emit dynamic routing information (RIP, OSPF, etc.) except specially configured gateway devices. Proxy ARP is currently not supported.

3. Minimum Network Hook-up Requirements for Unsecured Systems

The requirements listed below are the minimum requirements which must be satisfied before a new host can be installed on the unsecured subdomain of the company.com network as a unsecured system.

3.1. Designation of Support Group or Responsible Person

Each computer installed on the unsecured subdomain of the company.com network must have an assigned group or individual who provides full administrative support for the system and is responsible for ensuring the requirements of this policy are met. In addition, the responsible person or group ensures that the security of the system is maintained to meet minimum NASA, AMES and DPI security policies (See reference in introduction of this policy). If the responsible person is not reachable in the event of a major security problem, then the system will be powered down until approval to return to service is given by the DPI-CSO.

3.2. Notification of New System Installation

The appropriate personnel must be notified each time a new host is added to company.com network. The group of appropriate personnel includes the <COMPANY NAME> DPI-CSO, the <COMPANY NAME> CSA, the <COMPANY NAME> Network support group, and in most cases, the <COMPANY NAME> WKS support group. Prior to installation on the network, a valid IP address number must be assigned by the Network Operations Group. An IP address number can be obtained by sending email or leaving voice mail for the Network Operations Group. As part of the IP address request, the requestor must specify the new host as <COMPANY NAME>-secured or unsecured. If the system is designated as "unsecured", the Network Operations Group must first verify the request with the DPI-CSO prior to assigning a network IP address. The support status of the systems (e.g. "<COMPANY NAME>-secured" or "unsecured") must be included when the notification is posted to the nas.nets newsgroup, by the Network Support Group. In addition to posting a notice to the ops newsgroup, the Network Operations Group will be responsible for sending an email message, containing the same information as the news posting, to the mail alias. All other appropriate <COMPANY NAME> support personnel (e.g., WKS group, HSP group, etc.) will be responsible for reading the nas.nets news group on a regular basis (e.g., daily or several times a week).

3.3. Root Access

The passwords for all special/privileged accounts on unsecured systems will be provided to the <COMPANY NAME> CSA. All password changes for root and other special accounts must be reported to the <COMPANY NAME> CSA. Periodic system access checks will be made to ensure conformance (e.g, the <COMPANY NAME> CSA will attempt to log into the account using the password which was given.) All accounts on the system must have a password.

3.4. Standard <COMPANY NAME> Network Parameters

All hosts in the company.com domain must obtain a valid network number from the Network Operations group. The<COMPANY NAME> uses a subnetted class B address, netmask 255.255.255.0. The configured broadcast address for all <COMPANY NAME> hosts uses all ones for the host portion (e.g. 129.99.23.255). No host on the network should emit dynamic routing information (RIP, OSPF, etc.) except specially configured gateway devices. Proxy ARP is currently not supported.

3.5. Verification of Unsecured Systems

All unsecured systems must undergo a minimum security verification process prior to connection to the unsecured subnet of the company.com network. The <COMPANY NAME> Security Checklist, discussed in Chapter 13 of the <COMPANY NAME> System Administration Guide, will be used as a baseline for security. In addition, the <COMPANY NAME> CSA, or someone designated by the <COMPANY NAME> CSA, will be responsible for verifying that conditions outlined in this policy have been met, as well as any additional conditions specified by the <COMPANY NAME> DPI-CSO. Initial verification by the <COMPANY NAME> CSA will be made in a reasonable time frame. Re-verification can be done at any time by the <COMPANY NAME> CSA or someone they designate. Re-verification will be done periodically.

3.6. Recommended Requirements

In addition to the above listed requirements, it is recommended that users/owners of unsecured systems follow the <COMPANY NAME> standard for assignment of UIDs/GIDs and that they run the available security utilities used on <COMPANY NAME>-secured systems. The <COMPANY NAME> security utilities are discussed in Chapter 13 of the <COMPANY NAME> System Administration Guide

Approved by:

Concurrence:

Sample Escalation Procedures for Security Incidents

This procedure describes the steps which are to be taken for physical and computer security incidents which occur within the <COMPANY NAME> facility. The physical security incidents covered in this procedure are: theft (major and minor), illegal building access and property destruction (major or minor). The computer security incidents covered in this procedure are: loss of personal password sheet, suspected illegal system access (includes account sharing), suspected computer break-in (both internal and external) and computer viruses. For additional information on incident response and handling refer to the "<COMPANY NAME> Security Incident Handling Procedures." The types of incidents have been classified into three levels depending on severity. The Level One incidents are least severe and should be handled within one working day after the event occurs. Level One incidents usually require that only the <COMPANY NAME> Computer Security Officer and/or the <COMPANY NAME> Security Analyst be contacted. Level Two incidents are more serious and should be handled the same day the event occurs (usually within two to fours hours of the event). Level Two incidents must be escalated to the <COMPANY NAME> ISO and possibly some outside groups such as the CIAC or CERT. Level Three incidents are the most serious and should be handled as soon as possible.

LIST OF TERMS:

ISO - Installation Security Officer
CSO - Computer Security Officer
CSA - Computer Security Analyst
LSA - Lead System Analyst
NASIRC - NASA Computer Incident Response Center

List of Contacts

Computer Security Incidents1) Loss of Personal Password Sheet (Level One Incident)

A. Notify the <COMPANY NAME> CSA within one working day.

B. The <COMPANY NAME> CSA will decide if a password change is necessary.

2) Suspected Sharing of <COMPANY NAME> Accounts (Level One Incident)

A. **<COMPANY NAME>** User Services will document all pertinent information on a **<COMPANY NAME>** CMS report. If unable to contact **<COMPANY NAME>** CSA within two working days, disable appropriate accounts and inform the **<COMPANY NAME>** ISO and CSA.

B. The <COMPANY NAME> CSA will call person(s) suspected of account sharing and determine severeness of the incident. In most cases, people who share accounts have a valid need to have their own <COMPANY NAME> accounts. In these cases, the <COMPANY NAME> user's account will remain disabled until account request forms are received and process for the person who was using the <COMPANY NAME> user's account.

C. The <COMPANY NAME> CSA will escalate the issue to higher management if necessary.

3) Unfriendly Employee Termination (Level Two Incident)

A. Notify <COMPANY NAME> ISO and CSA within two hours. If neither can be reached within two hours, contact the backup CSA or ISO person.

B. Upon request from <COMPANY NAME> ISO or CSA, all <COMPANY NAME> accounts for terminated employee will be disabled by a member of System Control Accounts Section. At this point, members of System Control Section are not permitted to provide access (building or otherwise) to the terminated employee.

D. <COMPANY NAME> CSA will ensure building access is disabled and will confiscate card key, if possible.

E. If appropriate, the <COMPANY NAME> CSA will change systems passwords.

F. If necessary, the <COMPANY NAME> ISO will escalate issue to <COMPANY NAME> Division Office.

4) Suspected Violation of Special Access (Level Two Incident The misuse of Special Access is defined in the document "Special Access Guidelines Agreement" which is signed by each person having Special Access at <COMPANY NAME>.

Minor Violations - No threat to <COMPANY NAME> Security

A. Notify <COMPANY NAME> CSA within one working day. If unable to reach <COMPANY NAME> CSA within that time, contact the <COMPANY NAME> ISO or the backup person for the <COMPANY NAME> CSA. You should also inform the group leader and manager of the person suspected of violating the policy.

B. The <COMPANY NAME> CSA or designated backup will determine who is involved in the violation and the extent of the violation.

C. Notify the <COMPANY NAME> ISO within two working days.

D. If necessary, the NSA CSA will escalate issue to <COMPANY NAME> Division Office.

Major Violations - possible threat to <COMPANY NAME> and/or Ames security

A. Notify <COMPANY NAME> CSA within one hour. If neither can be reached within two hours, contact the backup person listed for the <COMPANY NAME> CSA.

B. Notify <COMPANY NAME> ISO within four hours. If he can not be reached within that time, contact his backup person.

C. If possible threat exists for Ames security, notify Ames ISO within 24 hours.

D. Disable all <COMPANY NAME> accounts for involved people.

E. Begin process of changing all system passwords.

F. Take further action as deemed necessary by <COMPANY NAME> CSA.

5) Suspected Computer Break-in or Computer Virus (Level Three Incident)

A. Isolate infected systems from the remaining <COMPANY NAME> network as soon as possible. The System Control Section support staff should consult the <COMPANY NAME> LAN/WAN teams to determine the best method to isolate the infected systems from the remaining <COMPANY NAME> network.

B. If a computer virus/worm is suspected, isolate <COMPANY NAME> network from outside networks as soon as possible. The <COMPANY NAME> LAN and WAN teams should be consulted before the disconnect takes place to discuss the best method and feasibility for doing a full disconnect from the Internet.

C. Notify <COMPANY NAME> CSA as soon as possible. If unable to reach him/her within ten minutes, contact the backup person.

D. Notify <COMPANY NAME> ISO within one hour. <COMPANY NAME> ISO will escalate to higher level management if necessary.

E. Notify all involved LSA's within two hours.

F. While waiting for LSA's and the <COMPANY NAME> CSA to respond, attempt to trace origin of attack and determine how many systems (if any) have been compromised. Save copies of system log files and any other files which may be pertinent to incident.

G. <COMPANY NAME> CSA will decide what further actions are needed and assign appropriate people to do perform the tasks.

H. The <COMPANY NAME> CSA will escalate the incident to the AMES AIS office, if necessary. Upon completion of the investigation, the <COMPANY NAME> CSA will write an incident summary report and submit to the appropriate levels of management.

Physical Security Incidents1) Illegal Building Access (Level Two Incident)

A. If during regular working hours an unauthorized person is in a controlled area, call or page the <COMPANY NAME> ISO immediately. If after working hours, call the Ames Security/Duty office first and then page the <COMPANY NAME> ISO or attempt to call his home phone number.

B. Escort the person outside the building or controlled area. Log incident and report to <COMPANY NAME> ISO.

C.The <COMPANY NAME> ISO and/or the Ames Security office will decide upon the appropriate action to take

2) Property Destruction or Personal Theft (Level Two or Three Incident)

A. Unless the theft or destruction is major, notify the <COMPANY NAME> ISO and <COMPANY NAME> CSA within one working day. If unable to reach <COMPANY NAME> ISO within one working day, contact the backup person listed on page one. Otherwise, for major theft or property destruction, notify <COMPANY NAME> ISO immediately. If he/she can not be reached within one hour, call or page the backup person.

B. Contact the Security Office within 24 hours.

C. If destruction involves a <COMPANY NAME> computer, notify LSA for that system within 24 hours.

D. If incident involves theft of <COMPANY NAME> property, contact the <COMPANY NAME> Property Custodian within two working days. The <COMPANY NAME> Property Custodian will contact the Property Custodian, if necessary. The <COMPANY NAME> ISO will escalate incident to <COMPANY NAME> Division Office as necessary.

Sample Incident Handling Procedure

1.0 INTRODUCTION

This document provides some general guidelines and procedures for dealing with computer security incidents. The document is meant to provide <COMPANY NAME> support personnel with some guidelines on what to do if they discover a security incident. The term incident in this document is defined as any irregular or adverse event that occurs on any part of the NPSN. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

* You see a strange process running and accumulating a lot of CPU time.
* You have discovered an intruder logged into your system.
* You have discovered a virus has infected your system.
* You have determined that someone from a remote site is trying to penetrate the system.

The steps involved in handling a security incident are categorized into five stages: protection of the system; identification of the problem; containment of the problem; eradication of the problem; recovering from the incident and the follow-up analysis. The actions taken in some of these stages are common to all types of security incidents and are discussed in section 2. Section 3 discusses specific procedures for dealing with worm/virus incidents and hacker/cracker incidents.

1.1 TERMS

Some terms used in this document are:

ISO - Installation Security Officer
CSO - Computer Security Officer
CSA - Computer Security Analyst
LSA - Lead System Analyst
CERT - Computer Emergency Response Team
CIAC - Computer Incident Advisory Capability

1.2 AREAS OF RESPONSIBILITY

In many cases, the actions outlined in this guideline will not be performed by a single person on a single system. Many people may be involved during the course of an active security incident which affects several of the <COMPANY NAME> systems at one time (i.e., a worm attack). The <COMPANY NAME> CSA should always be involved in the investigation of any security incident.

The <COMPANY NAME> ISO (put name here), the <COMPANY NAME> CSO (put name here) and the <COMPANY NAME> CSA (put name here) will act as the incident coordination team for all security-related incidents. In minor incidents, only the CSA will be involved. However, in more severe incidents all three may be involved in the coordination effort. The incident coordination team will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and clean-up are responsible for providing any needed information to members of the incident coordination team. Any directives given by a member of the incident coordination team will supersede this document.

1.3 IMPORTANT CONSIDERATIONS

A computer security incident can occur at anytime of the day or night. Although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be watching their flocks. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

The media is also an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge from a site currently responding to the incident. Providing information to the wrong people could have undesirable side effects. Section 2.3 discusses the policy on release of information.

2.0 GENERAL PROCEDURES

This section discusses procedures that are common for all types of security incidents.

2.1 KEEP A LOG BOOK

Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that can not be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted. The types of information that should be logged are:

* Dates and times of incident-related phone calls.
* Dates and times when incident-related events were discovered or occurred.
* Amount of time spent working on incident-related tasks.
* People you have contacted or have contacted you.
* Names of systems, programs or networks that have been affected.

2.2 INFORM THE APPROPRIATE PEOPLE

Informing the appropriate people is of extreme importance. There are some actions that can only be authorized by the <COMPANY NAME> ISO or CSO. <COMPANY NAME> also has the responsibility to inform other sites about an incident which may effect them. A list of contacts is provided below. Section 3 discusses who should be called and when for each type of security incident.

Phone numbers for the people below can be obtained from the <COMPANY NAME> Operations Manual in the <COMPANY NAME> Control Room. Also, the control room analysts can be of help when trying to contact the appropriate people.

List of Contacts

<COMPANY NAME> ISO -
Backup -
<COMPANY NAME> CSO -
Backup -
<COMPANY NAME> CSA -
Backup -
Ames Security/Duty Office –

2.3 RELEASE OF INFORMATION

Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. All release of information must be authorized by the <COMPANY NAME> ISO or by other people designated by the <COMPANY NAME> ISO. All requests for press releases must be forwarded to the Branch or Division level. Also, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be a security officer from another site. All suspicious requests for information (i.e., requests made by callers claiming to be a CSA for another site), should be forwarded to the <COMPANY NAME> CSO or Branch level. If there is any doubt about whether you can release a specific piece of information contact the <COMPANY NAME> CSO or <COMPANY NAME> ISO.

2.4 FOLLOW-UP ANALYSIS

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All on-line copies of infected files, worm code, etc., should be removed from the system(s). If applicable, a set of recommendations should be presented

to the appropriate management levels. A security incident report should be written by a person designated by the <COMPANY NAME> ISO and distributed to all appropriate personnel.

3.0 INCIDENT SPECIFIC PROCEDURES

This section discusses the procedure for handling virus, worm and hacker/cracker incidents.

3.1 VIRUS AND WORM INCIDENTS

Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes, thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, then proceed as if the attack was worm related.

3.1.1 Isolate the System

Isolate infected system(s) from the remaining <COMPANY NAME> network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the <COMPANY NAME> from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since <COMPANY NAME> will be disconnected from sites which may have patches. The <COMPANY NAME> ISO must authorize the isolation of the <COMPANY NAME> network from the outside world. **Log all actions.**

Do not power off or reboot systems that may be infected. There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.

3.1.2 Notify Appropriate People

Notify the <COMPANY NAME> CSA as soon as possible. If unable to reach him/her within 10 minutes, contact the backup person. The <COMPANY NAME> CSA will then be responsible for notifying other appropriate personnel. *** **NOTE -** Below, different times are given for suspected worm attack and for a suspected virus attack.

- The <COMPANY NAME> CSA will notify the <COMPANY NAME> CSO as soon as possible. If unable to reach him within one hour (10 minutes for a worm attack), his backup person will be contacted.
- The <COMPANY NAME> CSA or CSO will notify the <COMPANY NAME> ISO within two hours (one hour for a worm attack). The <COMPANY NAME> ISO will escalate to higher level management if necessary.
- The control room or <COMPANY NAME> CSA should notify all involved LSAs within four hours (two hours for a worm attack).

3.1.3 Identify the Problem

Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a snapshot of the system should be taken and saved. Below is a list of tasks to make a snapshot of the system:

1) Save a copy of all system log files. The log files are usually located in /usr/adm.
2) Save a copy of the root history file, */.history*.
3) Save copies of the */etc/utmp* and */etc/wtmp* files. Sometimes these files are found in the */usr/adm* directory.
4). Capture all process status information in a file using the command ps -awwxl > file name for BSD systems and ps -efl > file name for SYSV systems.

If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snap-shot information on the system.

Run the cops security checker on the infected system(s) to identify other possible problems such as altered system files, new suid programs or hidden special files. It may be necessary to install a clean version of cops from tape.

If other sites have been involved at this point, they may have helpful information on the problem and possible short term solutions. Also, any helpful information gained about the virus or worm should be passed along to Internet CERT sites, after approval by <COMPANY NAME> ISO. Log all actions.

3.1.4 Contain the virus or worm

All suspicious processes should now be halted and removed from the system. Make a full dump of the system and store in a safe place. The tapes should be carefully labeled so they will not be used by unsuspecting people in the future. Then remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all <COMPANY NAME> systems have been inoculated and/or the other internet sites have been cleaned up and inoculated. **Log all actions.**

3.1.5 Inoculate the System(s)

Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, then the tasks of assessing the damage is not very difficult. However, if the offending code has not been analyzed, then it may be necessary to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. **Log all actions.**

3.1.6 Return to a Normal Operating Mode

Prior to bringing the systems back into full operation mode, you should notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. **Log all actions.**

3.1.7 Follow-up Analysis

Perform follow-up analysis as described section 2.4.

3.2. HACKER/CRACKER INCIDENTS

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naive young students looking for a thrill. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to the NPSN.Hacker incidents can be divided into three types: attempts to gain access to a system, an active session on a system, or events which have been discovered after the fact. Of the three, an active hacker/cracker session is the most severe and must be dealt with as soon as possible. There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state (see section 3.2.2). The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information that will lead to a identification and possible criminal conviction (see section 3.2.3). The method used to handle a cracker/hacker incident will be determined by the level of understanding of the risks involved.

3.2.1 Attempted Probes into a NPSN System

Incidents of this type would include: repeated login attempts, repeated ftp, telnet or rsh commands, and repeated dial-back attempts.

3.2.1.1 Identify Problem

Identify source of attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such a system logs files, the root history file, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. **Log all actions.**

3.2.1.2 Notify <COMPANY NAME> CSA

Notify the <COMPANY NAME> CSA within 30 minutes. If the <COMPANY NAME> CSA can not be reached then notify the <COMPANY NAME> CSO or the <COMPANY NAME> CSA backup person. The <COMPANY NAME> CSA or their backup person will be responsible for notifying other levels of management.

3.2.1.3 Identify Hacker/Cracker

If the source of the attacks can be identified, then the <COMPANY NAME> CSA (or a designated person) will contact the system administrator or security analyst for that site and attempt to obtain the identify of the hacker/cracker. The NIC may be one source for obtaining the name and phone number of the site administrator of the remote site. If the hacker/cracker can be identified, the information should be provided to the <COMPANY NAME> CSO or ISO. The <COMPANY NAME> CSO or ISO will provide directions on how to proceed, if necessary. **Log all actions.**

3.2.1.4 Notify CERT

If the source of the attacks can not be identified, then the <COMPANY NAME> CSA will contact the Internet CERT and CIAC teams and provide them with information concerning the attack. ***NOTE - Release of information must be approved by the <COMPANY NAME> ISO or someone he designates. **Log all actions.**

3.2.1.5 Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the <COMPANY NAME> CSA or CSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

3.2.2 Active Hacker/Cracker Activity

Incidents of this type would include any active session or command by an unauthorized person. Some examples would include an active rlogin or telnet session, an active ftp session, or a successful dial-back attempt. In the case of active hacker/cracker activity, a decision must be made whether to allow the activity to continue while you gather evidence or to get the hacker/cracker off the system and then lock the person out. Since a hacker can do damage and be off the system in a matter of minutes, time is critical when responding to active hacker attacks. This decision must be made by the <COMPANY NAME> ISO or someone he designates (i.e., the <COMPANY NAME> CSO). The decision will be based on the availability of qualified personnel to monitor and observe the hacker/cracker and the level of risk involved.

3.2.2.1 Notify Appropriate People

Notify the <COMPANY NAME> CSA as soon as possible. If unable to reach him/her within 5 minutes, contact the backup person. The <COMPANY NAME> CSA will then be responsible for notifying other appropriate personnel. The <COMPANY NAME> CSA, with possible help from the involved LSA, will be responsible for trying to assess what the hacker/cracker is after and the risks involved in letting the hacker/cracker continue his/her activity.

The <COMPANY NAME> CSA will notify the <COMPANY NAME> CSO as soon as possible. If unable to reach him within ten minutes, his backup person should be contacted. The <COMPANY NAME> CSO can make the decision to allow the hacker to continue or to lock him out of the system. Based on the decision, follow the procedures in 2.1 or 2.2 below.

The <COMPANY NAME> CSA or CSO will notify the <COMPANY NAME> ISO within 30 minutes. The <COMPANY NAME> ISO will escalate to higher level management if necessary.

3.2.3 Removal of Hacker/Cracker From the System

3.2.3.1 Snap-shot the System

Make copies of all audit trail information such as system logs files, the root history files, the utmp and wtmp files, and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Any suspicious files should be moved to a safe place or archived to tape and then removed from the system. Also, get a listing of all active network connections. A control room analyst can provide assistance in obtaining snap-shot information on the system. **Log all actions.**

3.2.3.2 Lock Out the Hacker

Kill all active processes for the hacker/cracker and remove any files or programs that he/she may have left on the system. Change passwords for any accounts that were accessed by the hacker/cracker. At this stage, the hacker/cracker should be locked out of the system. **Log all actions.**

3.2.3.3 Restore the System

Restore the system to a normal state. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the log book for this incident. **Log all actions.**

3.2.3.4 Notify Other Agencies

by the <COMPANY NAME> ISO or someone he designates. **Log all actions**.

3.2.3.5 Follow-up

After the investigation, a short report describing the incident and actions that were taken should be written by the <COMPANY NAME> CSA or CSO and distributed to the appropriate people. Perform the follow-up analysis as described in section 2.4.

3.2.4 Monitoring of Hacker/Cracker Activity

There are no set procedures for monitoring the activity of a hacker. Each incident will be dealt with on a case by case basis. The <COMPANY NAME> ISO or the person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system(s), the steps outlined in section 3.2.3 above should be followed.

3.2.5 Evidence of Past Incidents

In the case of where an incident is discovered after the fact, there is not always a lot of evidence available to identify who the person was or how they gained access to the system. If you should discover that someone had successfully broke into a <COMPANY NAME> system, notify the <COMPANY NAME> CSA within one working day. The <COMPANY NAME> CSA will be responsible for notifying the appropriate people and investigating the incident.

Sample Partner Connection Policy

Object: To ensure that a secure method of connectivity is provided between <Company Name> and all third party (partnering) companies and to provide a formalized method for the request, approval and tracking of such connections.

Scope: This policy applies to all new third party connection requests and any existing third party network connections. In cases where existing third party network connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed.

Definition: A "third party network connection" is defined as one of the connectivity options listed in Section B. below. Third party companies can be <Company Name> Partners, Vendors and Suppliers.

A. Third-Party Connection Requests and Approvals
All requests for third party connections must be made using the Clarify problem tracking system, ISSU. The resulting ISSU case will be assigned to the appropriate network support team . A web-based case generation form will be established to help automate the process and to ensure the all correct information is submitted at the time of the request. The required information is outlined in Third Party Connection Request - Information Requirements Document. All information requested on this form must be completed prior to approval and sign off.

All third-party connection requests must have a VP level signature for approval. In some cases approval may be given at a lower level with pre-authorization from the appropriate VP. Also, all partnering companies must complete at sign any <Company Name> paperwork, such as NDA's as required by the <Company Name> Legal Department.

As a part of the request and approval process, the technical and administrative contact for the partnering company will be required to read and sign the Third Party Connection Acceptable Use Policy andany additional forms, such as Non-disclosure Agreements (NDAs), as required by the <Company Name> Legal Department.

B. Connectivity Options
The following five connectivity options are the standard methods of providing a third party/partner network connection. Anything that deviates from this standard must have a waiver sign-off at the VP level.

1) Leased line (e.g. T1) - Leased lines for partnering companies will be terminated on the Partners Subnet.

2) ISDN/FR - Dial leased lines will terminate on a partners only router located on the Partners subnet. Authentication for these connections must be as stated in Section E. below.

3) Encrypted Tunnel - Encrypted tunnels should be terminated on the Partners Subnet whenever possible. In certain circumstances, it may be required to terminate the encrypted tunnel on the dirty subnet, in which case the normal <Company Name> perimeter security measures will control access to internal devices.

4) Telnet access from Internet - Telnet access from the Internet will be provided by first telneting to the Partner gateway machine, where the connection will be authenticated per Section E. below. Once the connection is authenticated, telnet sessions to internal hosts will be limited to those services needed by using the authorization capabilities of <Company Name>Secure.

5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Partners modem pool. The connection will be authenticated per Section E. below.

C. Partner Access Points
When possible, Partner Access Points (PAPs) should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with leased line, Frame Relay and/or ISDN capability.

D. Services Provided

In general, services provided over the third party/partner connections should be limited only to those services needed, and only to those devices (hosts, routers, etc) needed. Blanket access shall not be provided for anyone. The default stance will be to deny all access and then only allow those specific services that are needed. In no case shall the partner connection to <Company Name> be used as the Internet connection for the partnering company. The standard set of allowable services are listed below:

1) File exchange via ftp - Where possible, file exchange via ftp should take place on the existing <Company Name> ftp servers (ftp-eng.<Company Name>.com for engineering related work or ftp.<Company Name>.com for all other work).

2) Electronic mail exchange - Business related email exchange between <Company Name> and the third party partners may be conducted over the partner connection as needed. Mail from the third party/partner sites to non-<Company Name> addresses will not be allowed over the partner network connection.

3) Telnet Access - Telnet access will be provided to specific <Company Name> hosts as needed.
Employees from partnering companies will only be given accounts on the specific <Company Name> hosts that are needed. Where possible router ACLs will be used to limit the paths of access to other internal <Company Name> hosts and devices.

** NIS accounts are not to be established for employees at partnering companies who have accounts on <Company Name> hosts.

4) Web Resource Access - Access to internal web resources will be provided on an as-needed basis. Access to <Company Name>'s public web resources shall be accomplished via the normal Internet access for the partner company.

5) Access to CVS Repositories - Access to <Company Name> source code will be provided by using the remote VOB capability.

E) Authentication for Third Party/Partner Connections
Third party connections made via remote dial-up using PPP/SLIP or standard UNIX telnet over the Internet, will be authenticated using the Partners Authentication database and Token Access System. Currently, ELI is the token access system in use. A separate server will be established specifically for third party companies. Reports, showing who has access via and ELI Gold card or softoken will be generated monthly and sent to the <Company Name> POCs for each partner company for verification and review.

Telnet connection made via the Internet must be initiated to a separate server (not the standard one) which authenticates to the Partners Authentication database and Token Access System mentioned above. The standard system will only be used for <Company Name> employees and contractors.

ISDN/FR connections will be authenticated via the Partners <Company Name>Secure database, which is separate from the <Company Name> ISDN authentication database.

F) <Company Name> Equipment at Third Party/Partner Sites
In many cases it may be necessary to have <Company Name>-owned and maintained equipment at the partnering site. All such equipment will be documented on the Third Party Connection Request - Information Requirements Document. Access to network devices such as routers and switches will only be provided to <Company Name> support personnel. All <Company Name>-owned equipment located at partnering sites is to be used for business purposes only. Any misuse of access or tampering with <Company Name> provided hardware will result in termination of the connection agreement between said parties.

G) Protection of Company Private Information and Resources
The network support group responsible for installation and configuration of a specific partner connection will be responsible for ensuring all possible measures have been taken to ensure the integrity and privacy of <Company Name> confidential information. At no time should <Company Name> rely on access/authorization control mechanisms at the partner site to protect or prohibit access to <Company Name> confidential information.

It shall not be <Company Name>'s responsibility to ensure the protection of the partnering company's information. The partnering company owns the responsibility to provide the appropriate security measures to ensure protection of their private Internetwork and Information.

H) Audit and Review of Third Party/Partner Connections

All aspects of third party partner connections will be monitored by the appropriate network support group. Where possible automated tools will be used to accomplish the auditing tasks. Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate <Company Name> POC. Each <Company Name> Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his area. Copies of the reports will also be mailed to the department directors.

Nightly audits will be performed on all partner router/network device configurations and the output will be mailed to the appropriate network support group. Any unauthorized changes will be investigatedimmediately.

All third party/partner connections will be reviewed on a quarterly bases and information regarding specific third party/partner connection will be updated as necessary. Obsolete partner connections will be terminated.

Sample Third Party Connection Acceptable Use Policy

Object: To ensure that a secure method of connectivity is provided between <Company Name> and all third party (partner) companies, and to provide guidelines for the use of network and computing resources associated with a Third Party Network as defined below.

Scope: This policy applies to all third party companies who form a partnership which <Company Name> which requires building a partner network. This includes the employees at said company who will be performing the work over the partner connection.

Definition: A "third party network connection" is defined as one of the connectivity options listed in Section B of the Partner Connection Policy. Third party companies can be <Company Name> Partners, Vendors and Suppliers.

Associated Documents:

Partner Connection Policy
Third Party Connection Request - Information Requirements Document

Third part network connections are to be used for business purposes only as outlined by the Information Requirements Document for each connection. Any violation of this Acceptable Use Policy may result in immediate termination of the connection/partner agreement with said parties.

In the text below, "user" refers to employees of the partner company who user the resources associated with the partner network.

1) The information provided on the Third Party Connection Request Information Requirements Document is correct to the best of my knowledge.

2) <Company Name> equipment located on partner premise will only be configured for TCP/IP and will only be used for <Company Name> related data transfers.

3) Configuration changes on <Company Name> equipment shall only be performed after notification and approval by the appropriate <Company Name> personnel.

4) The password on <Company Name> devices located on the partner premise will be set by a <Company Name> network engineer and is not to be changed unless approved by the appropriate <Company Name> personnel.

5) The partner company shall notify the appropriate <Company Name> personnel when an employee, who has access on <Company Name> equipment per the partner connection, leaves the company or is transferred to another position which no longer requires access.

6) The partner company shall assume all responsibility for protection of their private network(s) which may be interconnected vi the third party connection to <Company Name>.

7) Only employees of the partner company who have approved access shall use the resources associated with the partner connection. No sharing of accounts on <Company Name> owned and maintained devices will be permitted.

8) The point of contact at the partner company shall notify the appropriate <Company Name> personnel whenever there is a change in the user base for the work performed over the partner network.

9) The point of contact at the partner company shall notify the appropriate <Company Name> personnel whenever there is a changes in connection/function requirements of the partner network.

Any noncompliance with these requirements will constitute a security violation and will be reported to the appropriate <Company Name> Personnel, and it may result in immediate termination of the partner agreement.

I have read and understand the Third Party Connection Acceptable Use Policy for use of a third party partner connection and agree to abide by it.

---------- ----------

Requestor's Signature Date

Sample Third Party Connection Request
Information Requirements Document

In accordance with the Partner Connection Policy, all requests for third party/partner connections must be accompanied by this completed Information Requirements Document. This document should be completed by the person or group requesting the partners connection.

A. Requester Information

Name:
Department:
Manager's Name:
Director's Name:
Phone Number:
Email Address:

If requester is different from the technical contact, provide the above information for the technical contact person as well.

Also, please identify a backup point of contact and provide the appropriate information (Name, Phone number, Email address).

B. Problem Statement

What is the desired end result? You must include a statement about the business needs of the proposed connection.

C. Scope of needs

- What services are needed? (See Section D. of Partner's Policy)
- What are the privacy requirements (i.e. do you need encryption)?
- What are the bandwidth needs?
- How long is the connection needed?
- Future requirements, if any

D. Partner Company Information

- Technical contact (Name, Phone number, Email address)
- Backup Technical contact (Name, Phone number, Email address)
- Management contact (Name, Phone number, Email address)
- Location (address) of termination point of partner connection
- Host/domain names of Partner company
- Names (Email addresses, phone numbers) of all employees at partnering company who will use this access.

E. What type of work will be done over the partner connection? What applications will be used?

F Are there any known issues such as special services required? Are there any unknowns at this point, such as what internal <Company Name> services are needed?

G. Is a backup connection needed? (e.g., are there any critical business needs associated with this connection?)

H. What is the requested installation date?

I. What is the approximate duration of the partner connection?

J. Have Non-Disclosure agreements been sign with the partner company and/or the appropriate employees of the partner company?

K. Are there any exiting partner connections at <Company Name> with this company?

L. Other useful information.

Sample Partner Connection Migration Worksheet

The purpose of this worksheet is to provide a consistent documentation base for all new and existing partner connections. The information contained on this worksheet should be completed by the network engineer as the connection is undergoing migration. All information should be completed before the connection becomes production level.

This worksheet assumes the requester has completed the Information Requirements Document as outlined in the Third party/Partners Connection Policy. If not, you will need to have them complete it before work can proceed.

1) Equipment Needed:
a. List all equipment needed for this connection set-up.

b. Who will be purchasing equipment? Will it be charged back to the requester?

c. Which items will be located on Partner's premise?

d. Where will the hardware located at <Company Name>? Specify data center, rack and row. Please label equipment with the Partner's company name.

2) Address Space Requirements:
a. Would RFC1918 addresses be appropriate for this connection?

b. If so, can agreement be made on what is the best address space to use?

c. If RFC1918 addresses are used, is address translation required in both directions or just one?

d. Would a PIX box be appropriate for this connection?

3) Routing Requirements:
a. What address space needs to be routed.

b. Specify the static routes that will be used on all associated devices for this connection.

4) Physical Layout of the Connection:
a. Where does the connection terminate on the <Company Name> side. Provide circuit and BRI numbers where appropriate.

b. Where does the connection terminate on the Partner side. Provide circuit and BRI numbers where appropriate.

c. Provide a diagram of the connection.

5) Access to <Company Name> Devices and Services: (This information should be provided on the Third Party Connection Requirements Document. Please list here as well.)
a. What specific devices (hosts, network devices) must be accessed?

b. What services on those devices are needed?

5) Access Control Mechanisms:
a. How will access control be accomplished (ACLs on the routers, static routes, etc)? Where do the ACLs exist?

b. If access lists are used, what sequence numbers will be used for this connection. Remember that ACL sequence numbers should be unique for each partner and you should log both permits and denied on each end.

6) Administrative Information:
a. Is remote shell capability set up? If so, to where?

b. Where will logging information be sent?

* Before the connection is brought up to production state, the requester must specify which <Company Name> resources are needed and the proper access control mechanisms must be put in place.